Claims

[c1] 1.A method comprising:

receiving encrypted data from a client over an unsecure network in a first hop;

decrypting the encrypted data into decrypted data;

performing a test relative to the decrypted data, the test yielding one of at least a first result and a second result; and,

in response to the test yielding the first result, sending the decrypted data to an origin server over a given network in a second hop.

[c2] 2.The method of claim 1, wherein performing the test relative to the decrypted data comprises examining the decrypted data for security purposes, such that the first result is the decrypted data not presenting the security risk.

[c3] 3.The method of claim 1, wherein sending the decrypted data to the origin server over the given network in the second hop comprises first encrypting the decrypted data into second encrypted data.

[c4] 4.The method of claim 1, wherein the given network is a secure network.

[c5] 5.The method of claim 4, wherein the decrypted data is sent to the origin server over the given network in the second hop in accordance with one of the hypertext transport protocol (HTTP), the post office protocol (POP), the wireless access protocol (WAP), and the Internet messaging access protocol (IMAP).

[c6] 6.The method of claim 1, wherein the given network is one of the unsecure network and a second unsecure network.

[c7] 7.The method of claim 1, wherein the encrypted data is received from the client over the unsecure network in the first hop within a secure socket layer (SSL) session.

[c8] 8.The method of claim 1, wherein the unsecure network is the Internet.

[c9] 9.The method of claim 1, wherein the origin server is an effective origin server.

[c10] 10.The method of claim 1, wherein the client is an effective client.

[c11] 11.The method of claim 1, wherein the method is performed by a proxy within the given network.

[c12] 12.The method of claim 1, wherein the method is performed by a firewall within the given network.

[c13] 13.A computer-readable medium having a computer program stored thereon for execution by a processor to perform the method of claim 1.

[c14] 14.A method comprising:
receiving unencrypted data from a client over a secure network in a first hop;
performing a test relative to the unencrypted data, the test yielding one of at least a first result and a second result; and,
in response to the test yielding the first result,
encrypting the unencrypted data into encrypted data;
sending the encrypted data to an origin server over an unsecure network in a second hop.

[c15] 15.The method of claim 14, wherein performing the test relative to the unencrypted data comprises examining the unencrypted data for security purposes, such that the first result is the unencrypted data not presenting the security risk.

[c16] 16.The method of claim 14, wherein the unencrypted data is received from the client over the secure network in the first hop in accordance with one of the post office protocol (POP), the Internet messaging access protocol (IMAP), the hypertext transport protocol (HTTP), and the wireless access protocol (WAP).

[c17] 17.The method of claim 14, wherein the encrypted data is sent to the origin server over the unsecure network in the second hop within a secure socket

layer (SSL) session.

[c18] 18.The method of claim 14, wherein the secure network is a carrier network.

[c19] 19.The method of claim 14, wherein the unsecure network is the Internet.

[c20] 20.The method of claim 14, wherein the client is a thin client.

[c21] 21.The method of claim 14, wherein the client is one of a: personal digital assistant (PDA) device, a laptop computer, a notebook computer, and a wireless phone.

[c22] 22.The method of claim 14, wherein the secure network is one of a wireless network and a wired network.

[c23] 23.The method of claim 14, wherein the client is an effective client.

[c24] 24.The method of claim 14, wherein the origin server is an effective origin server.

[c25] 25.The method of claim 14, wherein the method is performed by a proxy within the secure network.

[c26] 26.The method of claim 14, wherein the method is performed by a firewall within the secure network.

[c27] 27.A computer-readable medium having a computer program stored thereon for execution by a processor to perform the method of claim 14.

[c28] 28.A system comprising:
a client to send encrypted data over an unsecure network in a first hop;
a proxy within a secure network to receive the encrypted data and decrypt the encrypted data into decrypted data, the proxy sending the decrypted data over the secure network in a second hop in response to performing a test relative to the decrypted data yielding a particular response; and,
an origin server within the secure network to receive the decrypted data.

[c29] 29.The system of claim 28, wherein the client is an effective client

comprising:

a second client within a second secure network to send unencrypted data over the second secure network in an additional hop; and,

a second proxy within the second secure network to receive the unencrypted data, the second proxy encrypting the unencrypted data into the encrypted data and sending the encrypted data over the unsecure network in the first hop in response to performing a second test relative to the unencrypted data yielding a second particular response.

[c30] 30.The system of claim 28, wherein the client is an effective client comprising:

a second client to send second encrypted data over the unsecure network in an additional hop; and,

a second proxy to receive the second encrypted data and decrypt the second encrypted data into second decrypted data, the second proxy encrypting the second decrypted data into the encrypted data and sending the encrypted data over the unsecure network in the first hop in response to performing a second test relative to the unencrypted data yielding a second particular response.

[c31] 31.A system comprising:

a client to send unencrypted data over a secure network in a first hop;

a proxy within the secure network to receive the unencrypted data, the proxy encrypting the unencrypted data into encrypted data and sending the encrypted data over an unsecure network in a second hop in response to performing a test relative to the unencrypted data yielding a particular response; and,

an origin server to receive the encrypted data.

[c32] 32.The system of claim 31, where the origin server is an effective origin server comprising:

a second proxy within a second secure network to receive the encrypted data and decrypt the encrypted data into decrypted data, the second proxy

sending the decrypted data over the second secure network in an additional hop; and,

a second origin server within the second secure network to receive the decrypted data.

[c33] 33.A proxy comprising:

one or more communication components enabling the proxy to communicate over a first network and a second network;

a processor; and,

a computer-readable medium having a computer program stored thereon for execution by the processor to receive data that is originally encrypted or unencrypted from a client over the first network in a first hop and decrypt the data where the data was originally encrypted, perform a test relative to the data yielding one of at least a first result and a second result, and in response to the test yielding the first result, sending the data unencrypted to an origin server over the second network in a second hop where the data was originally encrypted, and sending the data unencrypted or encrypted to the origin server over the second network in a second hop where the data was originally unencrypted.

[c34] 34.The proxy of claim 33, wherein the first network is a secure network.

[c35] 35.The proxy of claim 33, wherein the second network is an unsecure network, such that sending the data to the origin server over the second network in the second hop comprises first encrypting the data.

[c36] 36.The proxy of claim 33, wherein the second network is a secure network.